Algebraic Aspects of a Rank Factorization Problem Arising in Vibration Analysis

Yacine Bouzidi[1], Roudy Dagher[2], Elisa Hubert[3], and Alban Quadrat[4]

[1] bouzidi.yacine@gmail.com
[2] Inria Lille – Nord Europe, France roudy.dagher@inria.fr
[3] University of Lyon, UJM-St-Etienne, LASPI, 42334 Saint-Etienne, France elisa.hubert@wanadoo.fr
[4] Inria Paris, Ouragan project-team, IMJ – PRG, Sorbonne University, France alban.quadrat@inria.fr

Abstract. This paper continues the study of a rank factorization problem arising in gear fault surveillance [10–13]. The structure of a class of solutions − important in practice − of the rank factorization problem is studied. We show that these solutions can be parametrized. Using module theory and computer algebra methods, the parameter space $\mathcal{P}$ is explicitly characterized and is shown to be the complementary of an algebraic set. Finally, a finite open cover of $\mathcal{P}$ is obtained and for each basic open subset of the cover of $\mathcal{P}$, a closed-form solution is characterized.

Keywords: Polynomial systems · Effective module theory · Demodulation problems · Gearbox vibration signals.

1 Introduction

Before stating the mathematical problem studied in this paper, we first introduce a few notations. Let $\mathbb{k}$ denote a field (e.g., $\mathbb{k} = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$), R a commutative ring, $R^{n\times m}$ the R-module (the $\mathbb{k}$-vector space if $R = \mathbb{k}$) formed by all the $n \times m$ matrices with entries in R, $U(R) := \{r \in R \mid \exists\, s \in R : \, r\, s = 1\}$ the group of units of R, $\mathrm{GL}_n(R) := \{U \in R^{n\times n} \mid \det(U) \in \mathrm{U}(R)\}$ the *general linear group* of invertible $n \times n$ matrices with entries in R, and I_n the $n \times n$ identity matrix of $\mathrm{GL}_n(R)$. If $A \in R^{r\times s}$, then we can consider the following *R-homomorphisms*

$$
\begin{aligned}
.A : R^{1\times r} &\longrightarrow R^{1\times s} \\
\lambda &\longmapsto \lambda\, A,
\end{aligned}
\qquad
\begin{aligned}
A. : R^{s\times 1} &\longrightarrow R^{r\times 1} \\
\eta &\longmapsto A\, \eta,
\end{aligned}
$$

and the following *R-modules* (the $\mathbb{k}$-vector spaces if $R = \mathbb{k}$):

$$
\begin{cases}
\mathrm{im}_R(.A) := R^{1\times r} A, \\
\ker_R(.A) := \{\lambda \in R^{1\times r} \mid \lambda\, A = 0\}, \\
\mathrm{coker}_R(.A) := R^{1\times s}/\mathrm{im}_R(.A),
\end{cases}
\qquad
\begin{cases}
\mathrm{im}_R(A.) := A\, R^{s\times 1}, \\
\ker_R(A.) := \{\eta \in R^{s\times 1} \mid A\, \eta = 0\}, \\
\mathrm{coker}_R(A.) := R^{r\times 1}/\mathrm{im}_R(A.).
\end{cases}
$$

Recall that A is said to have *full column* (resp., *full row*) *rank* if $\ker_R(A.) = 0$ (resp., $\ker_R(.A) = 0$). $A \in \Bbbk^{r \times s}$ has full row rank (resp., full column rank) iff it admits a *right* (resp., *left*) *inverse* $B \in \Bbbk^{s \times r}$, i.e., $A\,B = I_r$ (resp., $B\,A = I_s$).

Motivated by the application of *vibration analysis* to *gearbox fault surveillance* [2, 3], a new *demodulation* approach of *gearbox vibration signals* was developed in [10, 11]. It yielded the study of the following mathematical problem.

Rank factorization problem:
Let $D_1, \ldots, D_r \in \Bbbk^{n \times n} \setminus \{0\}$ and $M \in \Bbbk^{n \times m} \setminus \{0\}$ be such that $\mathrm{rank}_{\Bbbk}(M) \leq r$. Determine $-$ if they exist $-$ $u \in \Bbbk^{n \times 1}$ and $v_1, \ldots, v_r \in \Bbbk^{1 \times m}$ satisfying:

$$M = \sum_{i=1}^{r} D_i\, u\, v_i. \tag{1}$$

Note that (1) is a system formed by $m\,n$ polynomial equations in the $n + m\,r$ entries of u and of the v_i's. Thus, (1) belongs to the realm of algebraic geometry.

The rank factorization problem was first solved for $r = 1$ and $D_1 = I_n$ in [11], and then for $r = 2$ and $D_1 = I_n$ in [12]. In [13], the general problem was studied with the assumption that the row vectors v_i's are $\Bbbk$-linearly independent, i.e., that the matrix $v := (v_1^T \ \ldots \ v_r^T)^T$ has full row rank. This assumption, which is motivated by the application, made the characterization of this class of solutions possible using linear algebra methods. These results are reviewed in Section 2.

Based on *module theory* and *computer algebra* methods [7, 14, 17], the first goal of the paper is to develop the algorithmic aspects of the results presented in [13]. We then study the set formed by all the solutions (u, v) of (1) with full row rank matrices v. An important problem in practice is to know how the solutions can vary within the solution space. Hence, we develop the local study of the solution space by proving the existence of local closed-form solutions that can be computed by computer algebra methods. Finally, the existence of global solutions is investigated and we show that this problem is related to well-known difficult problems of module theory (e.g., least number of a generator set of an ideal, recognizing when a stably free module over certain localizations of a polynomial ring is free and if so, computing a basis of the free module) [7, 17].

2 The rank factorization problem

In this section, we state again results on the problem obtained in [13]. If we note

$$A(u) := (D_1\, u \ \ldots \ D_r\, u) \in \Bbbk^{n \times r}, \quad v := (v_1^T \ \ldots \ v_r^T)^T \in \Bbbk^{r \times m},$$

then (1) can be rewritten as the following factorization of M (*bilinear system*):

$$M = A(u)\, v. \tag{2}$$

Note that if $(u,\, v)$ is a solution of (2), then so is $(\lambda\, u,\, \lambda^{-1}\, v)$ for all $\lambda \in \Bbbk \setminus \{0\}$.

We also note that Problem (2) is solvable iff there exists $u \in \Bbbk^{n \times 1}$ such that:

$$\mathrm{im}_{\Bbbk}(M.) \subseteq \mathrm{im}_{\Bbbk}(A(u).). \tag{3}$$

Indeed, if (2) holds, then $\zeta \in \operatorname{im}_{\Bbbk}(M.)$ is of the form $\zeta = M\,\eta = A(u)\,(v\,\eta)$ for a certain $\eta \in \Bbbk^{m\times 1}$, which shows that (3) holds. Conversely, if there exists a vector $u \in \Bbbk^{n\times 1}$ such that (3) holds, then for $i = 1, \ldots, m$, the i^{th} column $M_{\bullet i}$ of M belongs to $\operatorname{im}_{\Bbbk}(A(u).)$, and thus, there exists $w_i \in \Bbbk^{r\times 1}$ such that $M_{\bullet i} = A(u)\,w_i$, which yields (2) with $v := (w_1 \;\ldots\; w_m)$.

Using (3), a necessary condition for the solvability of (2) is then:

$$\exists\, u \in \Bbbk^{n\times 1}, \quad l := \operatorname{rank}_{\Bbbk}(M) \leq \operatorname{rank}_{\Bbbk}(A(u)) \leq \min\{r, n\}. \tag{4}$$

Suppose that (2) is solvable with a full row rank matrix v. Then, v admits a right inverse $t \in \Bbbk^{m\times r}$, i.e., $v\,t = I_r$. Hence, (2) yields $A(u) = M\,t$, which yields

$$\operatorname{im}_{\Bbbk}(A(u).) \subseteq \operatorname{im}_{\Bbbk}(M.), \tag{5}$$

and thus, we have:

$$\operatorname{im}_{\Bbbk}(A(u).) = \operatorname{im}_{\Bbbk}(M.). \tag{6}$$

The existence of $u \in \Bbbk^{n\times 1}$ satisfying (6) is then equivalent to:

1. $D_i\,u \in \operatorname{im}_{\Bbbk}(M.)$ for $i = 1, \ldots, r$, i.e., (5).
2. $\operatorname{rank}_{\Bbbk}(A(u)) = l := \operatorname{rank}_{\Bbbk}(M)$, i.e., $\dim_{\Bbbk}(\operatorname{span}\{D_i\,u\}_{i=1,\ldots,r}) = l$, i.e.:

$$\dim_{\Bbbk}(\ker_{\Bbbk}(A(u).) = r - l.$$

Remark 1. If $r = l$, then the last condition becomes $\ker_{\Bbbk}(A(u).) = 0$, i.e., the $D_i\,u$'s are $\Bbbk$-linearly independent, which yields the uniqueness of the matrix v.

Remark 2. If $\operatorname{rank}_{\Bbbk}(M) = \operatorname{rank}_{\Bbbk}(A(u))$, then (3) is equivalent to (6). Using (4), it holds if $l = \operatorname{rank}_{\Bbbk}(M) = r$ or $l = n$.

In this paper, we shall focus on the study of (6), i.e., on the above Conditions 1 and 2. In particular, we shall get the solutions $(u, v_1, \ldots, v_r)$ of (2) which are such that the v_i's are $\Bbbk$-linearly independent. In the demodulation problems for gearbox vibration signals [10], each row vector v_i contains Fourier coefficients of a signal to be estimated. The hypothesis that v has full row rank amounts to saying that the time signals are $\Bbbk$-linearly independent, which is a fair hypothesis in practice. The general rank factorization problem, i.e., (5), is studied in [6].

Let us now state again the approach developed in [13] for studying (2). We first suppose that $\ker_{\Bbbk}(.M) \neq 0$ (if $\ker_{\Bbbk}(.M) = 0$, see Remark 3 below). Let $L \in \Bbbk^{p\times n}$ be a full row rank matrix whose rows define a basis of $\ker_{\Bbbk}(.M)$, i.e.:

$$\ker_{\Bbbk}(.M) = \operatorname{im}_{\Bbbk}(.L), \quad p := \dim_{\Bbbk}(\ker_{\Bbbk}(.M)) = n - \operatorname{rank}_{\Bbbk}(M) = n - l.$$

Hence, we get $L\,M = 0$, which yields $\operatorname{im}_{\Bbbk}(M.) \subseteq \ker_{\Bbbk}(L.)$. Using $\dim_{\Bbbk}(\ker_{\Bbbk}(L.)) = n - p = \operatorname{rank}_{\Bbbk}(M)$, we obtain $\ker_{\Bbbk}(L.) = \operatorname{im}_{\Bbbk}(M.)$. Hence, Condition 1 above is equivalent to $D_i\,u \in \ker_{\Bbbk}(L.)$ for $i = 1, \ldots, r$, i.e., to the following linear system:

$$N\,u = 0, \quad N := ((L\,D_1)^T \;\ldots\; (L\,D_r)^T)^T \in \Bbbk^{p\,r\times n}.$$

If $\ker_{\Bbbk}(N.) = 0$, then $u = 0$, $A(u) = 0$ and (6) is not satisfied since $M \neq 0$.

Let us now suppose that $\ker_{\Bbbk}(N.) \neq 0$ and let $Z \in \Bbbk^{n\times d}$ be a full column matrix whose columns define a basis of $\ker_{\Bbbk}(N.)$, where $d := \dim_{\Bbbk}(\ker_{\Bbbk}(N.))$. The vectors $u \in \Bbbk^{n\times 1}$ satisfying Condition 1 are then defined by:

$$\forall\, \psi \in \Bbbk^{d\times 1}, \quad u = Z\,\psi. \tag{7}$$

Remark 3. If $\ker_{\Bbbk}(.M) = 0$, i.e., $\mathrm{rank}_{\Bbbk}(M) = n$, then $\mathrm{im}_{\Bbbk}(M.) = \Bbbk^{n\times 1}$. Condition 1 is $D_i\,u \in \Bbbk^{n\times 1}$ for $i = 1, \ldots, r$, which is satisfied for all $u \in \Bbbk^{n\times 1}$ and yields $Z = I_n$. Equivalently, if we set $L := 0$, then $N = 0$, and thus, $Z = I_n$.

Using (7), Condition 2, i.e., $\mathrm{rank}_{\Bbbk}(A(u)) = l$, is then equivalent to characterize the set of all the $\psi \in \Bbbk^{d\times 1}$ which are such that:

$$\mathrm{rank}_{\Bbbk}(A(Z\,\psi)) = l \;\Leftrightarrow\; \dim_{\Bbbk}(\ker_{\Bbbk}(A(Z\,\psi).) = r - l. \tag{8}$$

Example 1. Let us consider the following matrices:

$$M = \begin{pmatrix} 3 & 5 \\ 4 & 7 \end{pmatrix}, \quad D_1 = I_2, \quad D_2 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}.$$

Then, $l := \mathrm{rank}_{\Bbbk}(M) = r := 2$, which by Remark 3 shows that $Z = I_2$. Hence, (6) holds for all $u = \psi = (\psi_1 \quad \psi_2)^T$ satisfying $\det(A(\psi)) = \psi_1\,\psi_2 \neq 0$.

Let $X \in \Bbbk^{n\times l}$ be a full column rank whose columns define a basis of $\mathrm{im}_{\Bbbk}(M.)$. Since $\mathrm{im}_{\Bbbk}(M.) = \mathrm{im}_{\Bbbk}(X.)$, there exist $T \in \Bbbk^{m\times l}$ and a unique matrix $Y \in \Bbbk^{l\times m}$ such that $X = M\,T$ and $M = X\,Y$. Hence, we get $X\,(I_l - Y\,T) = 0$, which yields $Y\,T = I_l$ because X has full column rank. In particular, Y has full row rank.

By construction, $D_i\,Z\,\psi \in \ker_{\Bbbk}(L.) = \mathrm{im}_{\Bbbk}(M.) = \mathrm{im}_{\Bbbk}(X.)$ for all $\psi \in \Bbbk^{d\times 1}$, which shows that there exists a unique matrix $W_i \in \Bbbk^{l\times d}$ such that $D_i\,Z = X\,W_i$ for $i = 1, \ldots, r$. If we set $B(\psi) := (W_1\,\psi \;\ldots\; W_r\,\psi) \in \Bbbk^{l\times r}$, then we obtain:

$$\forall\, \psi \in \Bbbk^{d\times 1}, \quad A(Z\,\psi) = X\,B(\psi). \tag{9}$$

Using the fact that X has full column rank, we get $\ker_{\Bbbk}(A(Z\,\psi).) = \ker_{\Bbbk}(B(\psi).)$. Hence, using (8), (6) holds iff there exists $\psi \in \Bbbk^{d\times 1}$ such that:

$$\dim_{\Bbbk}(\ker_{\Bbbk}(B(\psi).)) = r - l \;\Leftrightarrow\; \mathrm{rank}_{\Bbbk}(B(\psi)) = l.$$

Hence, (6) holds iff the following set

$$\mathcal{P} := \left\{\psi \in \Bbbk^{d\times 1} \mid \mathrm{rank}_{\Bbbk}(B(\psi)) = l\right\} \tag{10}$$

is not empty. In particular, if $r = l$, then $\mathcal{P} = \left\{\psi \in \Bbbk^{d\times 1} \mid \det(B(\psi)) \neq 0\right\}$.

Let us suppose that $\mathcal{P} \neq \emptyset$ and let us show how to characterize the solutions $(u,\, v)$ of (2). By construction, $u = Z\,\psi$ for $\psi \in \mathcal{P}$ and using (9), we get $A(Z\,\psi)\,v = X\,B(\psi)\,v = X\,Y$. Now, since X has full column rank, we obtain:

$$B(\psi)\,v = Y. \tag{11}$$

Since $\psi \in \mathcal{P}$, $B(\psi)$ admits a right inverse $E_\psi \in \Bbbk^{r \times l}$, i.e., $B(\psi)\, E_\psi = I_l$. Hence, if the matrix $C_\psi \in \Bbbk^{r \times (r-l)}$ is such that its columns define a basis of $\ker_{\Bbbk}(B(\psi).)$, i.e., $\ker_{\Bbbk}(B(\psi).) = \mathrm{im}_{\Bbbk}(C_\psi.)$, then all the solutions of (11) are given by:

$$\forall\, Y' \in \Bbbk^{(r-l)\times m}, \quad v = E_\psi\, Y + C_\psi\, Y'.$$

Note that $\det((E_\psi \quad C_\psi)) \neq 0$. Hence, v has full row rank iff $Y' \in \Bbbk^{(r-l)\times m}$ is chosen such that the matrix $(Y^T \; {Y'}^T)^T \in \Bbbk^{r \times m}$ has full row rank. If $r = l$, then we note that $C_\psi = 0$, which shows again that v is unique (see Remark 1).

Theorem 1 ([13]). *With the above notations, (6) holds iff the set $\mathcal{P}$ defined by (10) is not empty. If so, then*

$$\forall\, \psi \in \mathcal{P}, \quad \forall\, Y' \in \Bbbk^{(r-l)\times m}, \quad \begin{cases} u = Z\, \psi, \\ v = (E_\psi \quad C_\psi) \begin{pmatrix} Y \\ Y' \end{pmatrix}, \end{cases} \tag{12}$$

are solutions of (2). Moreover, v has full row rank iff the matrix $Y' \in \Bbbk^{(r-l)\times m}$ is chosen such that $(Y^T \; {Y'}^T)^T \in \Bbbk^{r \times m}$ has full row rank. Finally, $\mathcal{P}$ does not depend on choices of the bases while defining the matrices L, Z and X.

Remark 4. Note that $0 \notin \mathcal{P}$ since $B(0) = 0$. If $\psi \in \mathcal{P}$ and $\lambda \in \Bbbk \setminus \{0\}$, then $B(\lambda\, \psi) = \lambda\, B(\psi)$, i.e., $\lambda\, \psi \in \mathcal{P}$. Remark 6 of [13] shows that the solutions (12) are stable under the transformations $(u,\, v) \longmapsto (\lambda\, u,\, \lambda^{-1}\, v)$ for all $\lambda \in \Bbbk \setminus \{0\}$.

Note that the matrices X, Y, Z, $W_1, \ldots, W_r$, B of Theorem 1 can be obtained by linear algebra methods as well as the matrices E_ψ and C_ψ for a fixed $\psi \in \mathcal{P}$.

Example 2. We consider again Example 1. Taking $X = M$ and $Y = I_2$, we get:

$$W_1 = \begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix}, \quad W_2 = \begin{pmatrix} 7 & -10 \\ -4 & 6 \end{pmatrix}, \quad B(\psi) = \begin{pmatrix} 7\,\psi_1 - 5\,\psi_2 & 7\,\psi_1 - 10\,\psi_2 \\ -4\,\psi_1 + 3\,\psi_2 & -4\,\psi_1 + 6\,\psi_2 \end{pmatrix},$$
$$\mathcal{P} = \{\psi \in \Bbbk^{2\times 1} \mid \det(B(\psi)) = \psi_1\, \psi_2 \neq 0\}, \quad C_\psi = 0,$$
$$E_\psi = \frac{1}{\psi_1\, \psi_2} \begin{pmatrix} -4\,\psi_1 + 6\,\psi_2 & -7\,\psi_1 + 10\,\psi_2 \\ 4\,\psi_1 - 3\,\psi_2 & 7\,\psi_1 - 5\,\psi_2 \end{pmatrix}.$$

Hence, the solutions of (2) are then defined by $u = \psi \in \mathcal{P}$ and $v = E_\psi$.

For more explicit examples, see [12, 13].

3 Characterization of $\mathcal{P}$

In this section, we characterize the set $\mathcal{P}$ defined by (10). An element $\psi \in \mathcal{P}$ is such that at least one of the $C_r^l := r!/(l!\,(r-l)!)$ $l \times l$-minors $\mathbb{m}_k(\psi)$ of the matrix $B(\psi) := (W_1\, \psi \; \ldots \; W_r\, \psi) \in \Bbbk^{l \times r}$ does not vanish, i.e., we have:

$$\mathcal{P} = \Bbbk^{d\times 1} \setminus \left\{\psi \in \Bbbk^{d\times 1} \mid \mathbb{m}_k(\psi) = 0,\ k = 1, \ldots, C_r^l\right\}. \tag{13}$$

Note that $\mathbb{m}_k$ is either 0 or a *homogeneous polynomial of degree* l, i.e., it satisfies $\mathbb{m}_k(\lambda\,\psi) = \lambda^l\,\mathbb{m}_k(\psi)$ for all $\lambda \in \mathbb{k} \setminus \{0\}$. Note also that C_r^l can be very large. Hence, we have to find a more tractable way to characterize $\mathcal{P}$.

If ψ is considered as an arbitrary vector of $\mathbb{k}^{d\times 1}$, then $B(\psi)$ can be interpreted as a matrix with polynomial entries in the ψ_i's. A natural framework for the study of $\mathcal{P}$ is thus *module theory* over a polynomial ring [7, 14]. Based on module theory and computer algebra methods (*Gröbner bases*) [7, 9, 17], in this section, we give a characterization of $\mathcal{P}$ which is more tractable in practice. The corresponding algorithm is implemented in the OREMODULES package [5] but the `homalg` library (GAP) [1] or the `Singular` system [9] can also be used.

Let $R := \mathbb{k}[x_1, \ldots, x_d]$ be the commutative polynomial ring in $x_1, \ldots, x_d$ with coefficients in the field $\mathbb{k}$. Moreover, let us consider:

$$x := (x_1 \ \ldots \ x_d)^T, \quad B := (W_1\,x \ \ldots \ W_r\,x) \in R^{l\times r}.$$

Then, we can define the following *finitely presented* R-module [7, 17]:

$$\mathcal{N} := \operatorname{coker}_R(B.) = R^{l\times 1}/\operatorname{im}_R(B.) = R^{l\times 1}/\left(B\,R^{r\times 1}\right).$$

The R-module $\mathcal{N}$ defines the obstruction of the surjectivity of the R-homomorphism $B. : R^{r\times 1} \longrightarrow R^{l\times 1}$, i.e., the obstruction for $B\,R^{r\times 1}$ to be equal to $R^{l\times 1}$.

Remark 5. In Remark 5 of [13], it is shown that, up to invertible matrices, B does not depend on arbitrary choices for the matrices L, X and Z (whose rows or columns define bases of certain $\mathbb{k}$-vector spaces). Hence, up to isomorphism, the R-module $\mathcal{N}$ is associated with the solvability of Problem (2).

We have the following *finite presentation* of the R-module $\mathcal{N}$ [7, 14, 17], i.e., the following *exact sequence* of R-modules:

$$0 \longleftarrow \mathcal{N} \xleftarrow{\kappa} R^{l\times 1} \xleftarrow{B.} R^{r\times 1}. \tag{14}$$

For each $\psi \in \mathbb{k}^{d\times 1}$, we can define the following *maximal ideal* of R

$$\mathfrak{m}_\psi := \langle x_1 - \psi_1, \ldots, x_d - \psi_d\rangle = \left\{ \sum_{i=1}^{d} a_i\,(x_i - \psi_i) \mid a_i \in R, \ i = 1, \ldots, d \right\}, \tag{15}$$

i.e., $R/\mathfrak{m}_\psi$ is isomorphic to the field $\mathbb{k}$, which is denoted by $R/\mathfrak{m}_\psi \cong \mathbb{k}$ [7, 14, 17].

Applying the *covariant right exact functor* $(R/\mathfrak{m}_\psi) \otimes_R \cdot$ to (14), we obtain the following exact sequence of $\mathbb{k}$-vector spaces [7, 17]:

$$0 \longleftarrow (R/\mathfrak{m}_\psi) \otimes_R \mathcal{N} \xleftarrow{\mathrm{id}\otimes\kappa} \mathbb{k}^{l\times 1} \xleftarrow{B(\psi).} \mathbb{k}^{r\times 1}. \tag{16}$$

Using properties of tensor products [17], $B(\psi). : \mathbb{k}^{r\times 1} \longrightarrow \mathbb{k}^{l\times 1}$ is surjective iff

$$\mathcal{N}/(\mathfrak{m}_\psi\,\mathcal{N}) \cong (R/\mathfrak{m}_\psi) \otimes_R \mathcal{N} \cong \mathbb{k}^{l\times 1}/\left(B(\psi)\,\mathbb{k}^{r\times 1}\right) = 0,$$

where $\mathfrak{m}_\psi \, \mathcal{N} := \left\{ \sum_{i \in I} a_i \, n_i \mid a_i \in \mathfrak{m}_\psi, \, n_i \in \mathcal{N}, \, \sharp I < \infty \right\}$, i.e., iff we have:

$$\mathcal{N} = \mathfrak{m}_\psi \, \mathcal{N}. \tag{17}$$

Note that $\mathfrak{m}_\psi \subset R$ yields $\mathfrak{m}_\psi \, \mathcal{N} \subset \mathcal{N}$, i.e., (17) is equivalent to $\mathcal{N} \subset \mathfrak{m}_\psi \, \mathcal{N}$, i.e.:

$$\mathcal{P} = \left\{ \psi \in \Bbbk^{d \times 1} \mid \mathcal{N} \subset \mathfrak{m}_\psi \, \mathcal{N} \right\}.$$

Nakayama's lemma [7, 14, 17] gives a necessary condition for (17). Before stating again this well-known result, we rewrite (17) in terms of equations. Let $\kappa : R^{l \times 1} \longrightarrow \mathcal{N}$ be the R-homomorphism which sends $\eta \in R^{l \times 1}$ onto its *residue class* in $\mathcal{N}$, i.e., $\kappa(\eta') = \kappa(\eta)$ if there exists $\zeta \in R^{r \times 1}$ such that $\eta' = \eta + B \, \zeta$ [17]. Let f_j be the j^{th} vector of the standard basis of $R^{l \times 1}$, i.e., the vector defined by 1 at the j^{th} position and 0 elsewhere, and $y_j := \kappa(f_j)$ the residue class of f_j in $\mathcal{N}$. It can be easily show that $\{y_j\}_{j=1,\ldots,l}$ is a set of generators of $\mathcal{N}$ [4, 16]. Then, (17) is equivalent to the existence of $r_{jk} \in \mathfrak{m}_\psi$ such that $y_j = \sum_{k=1}^{l} r_{jk} \, y_k$ for $j = 1, \ldots, l$. Noting $y := (y_1, \ldots, y_l)^T$, (17) is equivalent to the existence of $G := (r_{jk}) \in {\mathfrak{m}_\psi}^{l \times l}$ such that $(I_l - G) \, y = 0$, which is then equivalent to the existence of $E \in R^{r \times l}$ such that $I_l = G + B \, E$, and thus:

$$\mathcal{P} = \left\{ \psi \in \Bbbk^{d \times 1} \mid \exists \, G \in {\mathfrak{m}_\psi}^{l \times l}, \, \exists \, E \in R^{r \times l} : \; I_l = G + B \, E \right\}.$$

Setting $x := \psi$, $I_l = G + B \, E$ yields $B(\psi) \, E(\psi) = I_l$ and $\operatorname{rank}_{\Bbbk}(B(\psi)) = l$.

Now, if $(I_l - G)^{\text{adj}}$ denotes *adjugate matrix* of $I_l - G$, using the standard identity $(I_l - G)^{\text{adj}} \, (I_l - G) = \det(I_l - G)$ [17], then we get $\det(I_l - G) \, y = 0$. Let $p(\lambda) := \det(\lambda \, I_l - G) = \lambda^l + p_1 \, \lambda^{l-1} + \ldots + p_l$ be the characteristic polynomial of G. We can check that $p_i \in \mathfrak{m}_\psi$ for $i = 1, \ldots, l$, and thus, $\det(I_l - G) = p(1) = 1 + a$ for a certain $a \in \mathfrak{m}_\psi$. Since $1 \notin \mathfrak{m}_\psi$, $\det(I_l - G) \neq 0$ and each generator y_j of $\mathcal{N}$ satisfies the non-trivial equation $(1 + a) \, y_j = 0$ for $j = 1, \ldots, l$. Hence, we get

$$0 \neq 1 + a \in \operatorname{ann}_R(\mathcal{N}) := \{ b \in R \mid b \, \mathcal{N} = 0 \}, \tag{18}$$

where $\operatorname{ann}_R(\mathcal{N})$ is an ideal of R called the *annihilator* of $\mathcal{N}$. Nakayama's lemma asserts (17) implies (18) [7, 14, 17]. In particular, (18) implies that the R-module $\mathcal{N}$ is *torsion*, namely, $t(\mathcal{N}) := \{ n \in \mathcal{N} \mid \exists \, 0 \neq b \in R : \; b \, n = 0 \} = \mathcal{N}$ [7, 17].

Let us consider a family of generators $\{g_i\}_{i=1,\ldots,t}$ of $\operatorname{ann}_R(\mathcal{N})$, i.e.:

$$\operatorname{ann}_R(\mathcal{N}) = \langle g_1, \ldots, g_t \rangle := \left\{ \sum_{i=1}^{t} a_i \, g_i \mid a_1, \ldots, a_t \in R \right\}. \tag{19}$$

A set of generators $\{g_i\}_{i=1,\ldots,t}$ of $\operatorname{ann}_R(\mathcal{N})$ can be computed by the command PiPolynomial of OreModules [5]. See also `Homalg` [1] and `Singular` [9]. Note that t is usually much smaller than C_r^l. Now, (18) shows that there exist $q_i \in R$ for $i = 1, \ldots, t$ satisfying $1 + a = \sum_{i=1}^{t} q_i \, g_i$. Evaluating this identity at the point $x = \psi$, we obtain the following Bézout identity:

$$\sum_{i=1}^{t} q_i(\psi) \, g_i(\psi) = 1. \tag{20}$$

Hence, $\psi \in \Bbbk^{d \times 1}$ must to be chosen such that the generators $g_1, \ldots, g_t$ of $\mathrm{ann}_R(\mathcal{N})$ do not simultaneously vanish at ψ.

Remark 6. For two finitely generated R-modules $\mathcal{M}$ and $\mathcal{N}$, it can be proved that $\mathcal{M} \otimes_R \mathcal{N} = 0$ implies $\mathrm{ann}_R(\mathcal{M}) + \mathrm{ann}_R(\mathcal{N}) = R$. See, e.g., Corollary 4.9 of [7]. Setting $\mathcal{M} := R/\mathfrak{m}_\psi$ and using $\mathrm{ann}_R(\mathcal{M}) = \mathfrak{m}_\psi$, a necessary condition for $\psi \in \mathcal{P}$ is then $\mathfrak{m}_\psi + \mathrm{ann}_R(\mathcal{N}) = \langle x_1 - \psi_1, \ldots, x_d - \psi_d, g_1, \ldots, g_t \rangle = R$, i.e., $\sum_{i=1}^t q_i\, g_i + \sum_{j=1}^d r_j\, (x_j - \psi_j) = 1$ for certain $q_i, r_j \in R$, $i = 1, \ldots, t$, $j = 1, \ldots, d$, which, by evaluation at $x = \psi$, yields again the Bézout identity (20).

If I is an ideal of R, we can define the *algebraic set* of the *affine space* $\Bbbk^{d \times 1}$:

$$V_\Bbbk(I) := \{\psi \in \Bbbk^{d \times 1} \mid \forall\, g \in I: \; g(\psi) = 0\}.$$

If $I = \langle g_1, \ldots, g_t \rangle$, i.e., I is generated by the g_i's, then $V_\Bbbk(I)$ is the common zeros $\psi \in \Bbbk^{d \times 1}$ of all the g_i's, i.e., $V_\Bbbk(I) = \{\psi \in \Bbbk^{d \times 1} \mid g_i(\psi) = 0,\; i = 1, \ldots, t\}$. Hence:

$$V_\Bbbk(\mathrm{ann}_R(\mathcal{N})) = V_\Bbbk(\langle g_1, \ldots, g_t \rangle) = \bigcap_{i=1}^t V_\Bbbk(\langle g_i \rangle). \tag{21}$$

Hence, a necessary condition for (17) to hold is $\psi \in \Bbbk^{d \times 1} \setminus V_\Bbbk(\mathrm{ann}_R(\mathcal{N}))$. This condition is also sufficient as explained in the following remark.

Remark 7. Let $\mathrm{Fitt}_0(\mathcal{N})$ be the 0^{th} *Fitting ideal* of $\mathcal{N}$, namely, the ideal of R defined by all the $l \times l$-minors of B [7]. Proposition 20.7 of [7] then yields:

$$\mathrm{ann}_R(\mathcal{N})^l \subseteq \mathrm{Fitt}_0(\mathcal{N}) \subseteq \mathrm{ann}_R(\mathcal{N}).$$

If $\sqrt{I} := \{a \in R \mid \exists\, n \in \mathbb{Z}_{\geq 0}: \; a^n \in I\}$ denotes the *radical* of I [7, 14], then

$$\sqrt{\mathrm{ann}_R(\mathcal{N})} = \sqrt{\mathrm{Fitt}_0(\mathcal{N})} \;\Rightarrow\; V_\Bbbk(\mathrm{ann}_R(\mathcal{N})) = V_\Bbbk(\mathrm{Fitt}_0(\mathcal{N}))),$$

which also shows again (13), i.e., $\mathcal{P} = \Bbbk^{d \times 1} \setminus V_\Bbbk(\mathrm{Fitt}_0(\mathcal{N})))$.

In Section 4, we shall give a more useful proof of $\mathcal{P} = \Bbbk^{d \times 1} \setminus V_\Bbbk(\mathrm{ann}_R(\mathcal{N}))$.

Example 3. We consider the following matrices:

$$M = \begin{pmatrix} 0 & 0 \\ -147360 & -96804 \\ 0 & 0 \end{pmatrix}, \; D_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 54 & -31 \\ 0 & 0 & 0 \end{pmatrix},$$
$$D_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -58 & -77 \\ 0 & 0 & 0 \end{pmatrix}, \qquad D_3 = \begin{pmatrix} 0 & 0 & 0 \\ 79 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

We can check that $l := \mathrm{rank}_\Bbbk(M) = 1 < r = 3$,

$$X = \begin{pmatrix} 0 \\ -147360 \\ 0 \end{pmatrix}, \; Y = \begin{pmatrix} 1 & \frac{8067}{12280} \end{pmatrix}, \; L = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; N = 0, \; Z = I_3,$$

and $\psi = (\psi_1 \quad \psi_2 \quad \psi_3)^T$. If $c := 1/(147360)$, then we have:

$$W_1 = c\,(0 \quad -54 \quad 31)\,, \quad W_2 = c\,(0 \quad 58 \quad 77)\,, \quad W_3 = c\,(-79 \quad 0 \quad 0)\,,$$
$$B(\psi) = c\,(-54\,\psi_2 + 31\,\psi_3 \quad 58\,\psi_2 + 77\,\psi_3 \quad -79\,\psi_1)\,.$$

Let $R = \Bbbk[x_1, x_2, x_3]$, $x := (x_1 \quad x_2 \quad x_3)^T$, $B := (W_1\,x \quad W_2\,x \quad W_3\,x) \in R^{1\times 3}$. The R-module $\mathcal{N} = R/\left(B\,R^{3\times 1}\right) = R/I$, where $I = \langle B_1, B_2, B_3\rangle$ is the ideal generated by the three entries B_i's (i.e., 1×1-minors $\mathbb{m}_k$) of B, is clearly a torsion R-module. The R-module $\mathcal{N}$ is generated by the residue class y of 1 in $\mathcal{N}$ and we can check that $\mathrm{ann}_R(\mathcal{N}) = I = \mathfrak{m}_0 := \langle x_1, x_2, x_3\rangle$. Such a computation can directly be obtained by the PiPolynomial command of the OreModules package [5]. Hence, we get:

$$V_{\Bbbk}(\mathrm{ann}_R(\mathcal{N})) = \left\{(0\;0\;0)^T\right\} \;\Rightarrow\; \mathcal{P} = \Bbbk^{3\times 1} \setminus \{0\}.$$

Remark 8. Since the generators g_i's of $\mathrm{ann}_R(\mathcal{N})$ can be chosen to be homogeneous polynomials, $0 \in V_{\Bbbk}(\mathrm{ann}_R(\mathcal{N}))$, which shows that $0 \notin \mathcal{P}$ (see Remark 4).

4 Local & global studies of the solution space

4.1 Existence of a local/global right inverse *E* of *B*

Let us first study the problem of computing a right inverse E_ψ of $B(\psi)$ for $\psi \in \mathcal{P}$. With the notation (19), let us consider the following integral domain

$$S_{g_i}^{-1} R := \left\{ \frac{a}{g_i^n} \mid a \in R,\, n \in \mathbb{Z}_{\geq 0} \right\},$$

i.e., the *localization* of R at the *multiplicatively closed set* $S_{g_i} := \{g_i^n \mid n \in \mathbb{Z}_{\geq 0}\}$ [7, 14, 17]. We can then consider the *localization* of $\mathcal{N}$ with respect of the powers of g_i, namely, the $S_{g_i}^{-1}R$-module defined by $S_{g_i}^{-1}\mathcal{N} := \{s^{-1}\,n \mid s \in S_{g_i},\, n \in \mathcal{N}\}$. It is well-known $S_{g_i}^{-1}R$ is a *flat* R-module [7, 14, 17], which yields the isomorphism

$$S_{g_i}^{-1}\mathcal{N} \cong (S_{g_i}^{-1}R)^{l\times 1} / \left(B\,(S_{g_i}^{-1}R)^{r\times 1}\right)$$

of $S_{g_i}^{-1}R$-modules. Hence, $S_{g_i}^{-1}\mathcal{N}$ can be seen as the $S_{g_i}^{-1}R$-module obtained from $\mathcal{N}$ by extending the scalars from R to $S_{g_i}^{-1}R$. See, e.g., [7, 14, 17]. By definition (see (19)), we have $g_i\,\mathcal{N} = 0$ and $g_i^{-1} \in S_{g_i}^{-1}R$, which yields $S_{g_i}^{-1}\mathcal{N} = 0$, i.e.:

$$B\,(S_{g_i}^{-1}R)^{r\times 1} = (S_{g_i}^{-1}R)^{l\times 1}, \quad i = 1, \ldots, t.$$

Hence, there exists $E_{g_i} \in (S_{g_i}^{-1}R)^{r\times l}$ such that $B\,E_{g_i} = I_l$, i.e., E_{g_i} is a right inverse of B defined over the *Zariski distinguished/basic open subset* of $\Bbbk^{d\times 1}$ [7]

$$D(g_i) := \Bbbk^{d\times 1} \setminus V_{\Bbbk}(\langle g_i\rangle), \quad i = 1, \ldots, t,$$

i.e., $E_{g_i}(\psi)$ is a right inverse of $B(\psi)$ for all $\psi \in D(g_i)$, where $E_{g_i}(\psi)$ denotes the value of the matrix E_{g_i} evaluated at $x := \psi$. The matrix E_{g_i} can be computed by the LocalLeftInverse command of the OreModules package.

Remark 9. Using (14), we get the *split exact sequence* of $S_{g_i}^{-1}R$-modules [17]:

$$0 = S_{g_i}^{-1}\mathcal{N} \xleftarrow{S_{g_i}^{-1}\kappa} (S_{g_i}^{-1}R)^{l\times 1} \underset{B.}{\overset{E_{g_i}\cdot}{\rightleftarrows}} (S_{g_i}^{-1}R)^{r\times 1} .$$

Thus, we have $S_{g_i}^{-1}\operatorname{im}_R(B.) = \operatorname{im}_{S_{g_i}^{-1}R}(B.) \cong (S_{g_i}^{-1}R)^{l\times 1}$ for $i = 1, \ldots, t$, i.e., $S_{g_i}^{-1}R$-module $S_{g_i}^{-1}\operatorname{im}_R(B.)$ is free of rank l.

From the above results, $\operatorname{rank}_{\Bbbk}(B(\psi)) = l$ for all $\psi \in \Bbbk^{d\times 1} \setminus \bigcap_{i=1}^{t} V_{\Bbbk}(\langle g_i\rangle)$. Using (21), (2) has solutions in the complementary $\mathcal{P}$ of the Zariski closed subset $V_{\Bbbk}(\operatorname{ann}_R(\mathcal{N}))$ in $\Bbbk^{d\times 1}$. Hence, if $\mathcal{P} \neq \emptyset$ (e.g., $\operatorname{ann}_R(\mathcal{N}) \neq \langle 0\rangle$ and $\Bbbk$ is algebraically closed), then (2) *generically* has solutions in the sense of algebraic geometry, i.e., outside the Zariski closed subset $V_{\Bbbk}(\operatorname{ann}_R(\mathcal{N}))$ of $\Bbbk^{d\times 1}$ [7, 14]. Moreover, we have:

$$\begin{aligned}\mathcal{P} &= \Bbbk^{d\times 1} \setminus \bigcap_{i=1}^{t} V_{\Bbbk}(\langle g_i\rangle) = \bigcup_{i=1}^{t} \left(\Bbbk^{d\times 1} \setminus V_{\Bbbk}(\langle g_i\rangle)\right) = \bigcup_{i=1}^{t} D(g_i)\\ &= \left\{\psi \in \Bbbk^{d\times 1} \mid \exists\, i \in [\![1, \ldots, t]\!] : \psi \notin V_{\Bbbk}(\langle g_i\rangle)\right\}.\end{aligned}$$

Since $\mathcal{P} \cap D(g_i) = D(g_i)$, $D(g_i)$ is also an open subset of $\mathcal{P}$ for the induced *Zariski topology* [7, 14]. Finally, $\mathcal{P}$ is an open subset of the *irreducible* affine set $\Bbbk^{d\times 1} = V_{\Bbbk}(\langle 0\rangle)$, i.e., which shows that $\mathcal{P}$ is a *quasi-affine variety* [9].

Theorem 2. *Let $R = \Bbbk[x_1, \ldots, x_d]$, $x = (x_1 \ \ldots \ x_d)^T$, $W_i \in \Bbbk^{l\times d}$, $i = 1, \ldots, r$, be the matrices defined in Section 2, $B = (W_1\, x \ \ldots \ W_r\, x) \in R^{l\times r}$, the R-module $\mathcal{N} = R^{l\times 1}/\left(B\, R^{r\times 1}\right)$ and its annihilator $\operatorname{ann}_R(\mathcal{N}) = \langle g_1, \ldots, g_t\rangle$. Then, we get:*

$$\mathcal{P} = D(\operatorname{ann}_R(\mathcal{N})) := \Bbbk^{d\times 1} \setminus V_{\Bbbk}(\operatorname{ann}_R(\mathcal{N})). \tag{22}$$

Hence, Problem (2) has solutions in the complementary $\mathcal{P}$ of the closed algebraic set $V_{\Bbbk}(\operatorname{ann}_R(\mathcal{N}))$ in $\Bbbk^{d\times 1}$. Moreover, $\operatorname{ann}_R(\mathcal{N}) = \langle 0\rangle$ yields $\mathcal{P} = \emptyset$ and the converse holds if $\Bbbk$ is algebraically closed.

The quasi-affine variety $\mathcal{P}$ has a finite open cover *defined by $\mathcal{P} = \bigcup_{i=1}^{t} D(g_i)$, where $D(g_i) := \Bbbk^{d\times 1} \setminus V_{\Bbbk}(\langle g_i\rangle)$ is a basic open subset of $\Bbbk^{d\times 1}$ (of $\mathcal{P}$). Finally, there exist $E_{g_i} \in (S_{g_i}^{-1}R)^{r\times l}$ such that $B\, E_{g_i} = I_l$ for $i = 1, \ldots, t$, i.e., for each $D(g_i)$, there exists a smooth right inverse E_{g_i} of B, i.e., $\psi \in D(g_i) \longmapsto E_{g_i}(\psi)$.*

Using Theorem 2, $B(\psi)$ admits a global right inverse $E(\psi)$ over $\mathcal{P}$, i.e., $B(\psi)\, E(\psi) = I_l$ for all $\psi \in \mathcal{P}$, iff the ideal $\operatorname{ann}_R(\mathcal{N})$ can be generated by a single element $g \in R$, i.e., $\operatorname{ann}_R(\mathcal{N}) = \langle g\rangle$, in which case $\operatorname{ann}_R(\mathcal{N})$ is principal [7, 17]. For instance, it is the case if we have $l = r$ and $g := \det(B) \neq 0$ (see Example 2), or if $d = 1$, i.e., $R = \Bbbk[x_1]$ is a *principal ideal domain*, namely, every ideal of R (e.g., $\operatorname{ann}_R(\mathcal{N})$) can be generated by a single element g of R which can be obtained by Euclidean division [7, 17]. Let us now study the general case. Let $\operatorname{ann}_R(\mathcal{N}) = \langle g_1, \ldots, g_t\rangle$, g be a greatest common divisor of all the g_i's and $g_i' := g_i/g \in R$ for $i = 1, \ldots, t$. We then get $\operatorname{ann}_R(\mathcal{N}) = \langle g\rangle\langle g_1', \ldots, g_t'\rangle$, which shows that $\operatorname{ann}_R(\mathcal{N})$ is principal iff so is $\langle g_1', \ldots, g_t'\rangle$, i.e., iff $\langle g_1', \ldots, g_t'\rangle = R$, i.e., iff there exist $h_i \in R$ for $i = 1, \ldots, t$ such that $\sum_{i=1}^t h_i \, g'_i = 1$. If $\Bbbk = \mathbb{C}$, using *Hilbert's Nullstellensatz* [7, 14], this Bézout identity is equivalent to the fact that all the g'_i's have no common zeros in $\mathbb{C}^{d \times 1}$, which can be checked by a *Gröbner basis computation* [7, 9]. Now, using Remark 8, $0 \in V_{\mathbb{C}}\,(\mathrm{ann}_R(\mathcal{N})) = V_{\mathbb{C}}(\langle g \rangle) \bigcup V_{\mathbb{C}}(\langle g'_1, \ldots, g'_t \rangle)$, i.e., $g(0) = 0$ or $g'_i(0) = 0$ for all $i = 1, \ldots, t$. In particular, if $g = 1$, then $\mathrm{ann}_R(\mathcal{N})$ is not a principal ideal. Finally, if $\langle g'_1, \ldots, g'_t \rangle = R$, i.e., $\mathrm{ann}_R(\mathcal{N}) = \langle g \rangle$, then $g(0) = 0$.

The problem of finding the least number of generators $\mu(I)$ of an ideal I is a well-known difficult problem in module theory (see, e.g., [14, 15]). In our problem, $\mu(\mathrm{ann}_R(\mathcal{N}))$ is the least number of open sets $D(g_i)$'s which defines a finite open cover of $\mathcal{P}$. Since $\mathrm{ann}_R(\mathcal{N})$ is generated by homogeneous polynomials, it can be proved that $\mu\,(\mathrm{ann}_R(\mathcal{N})) = \mu\,\left(\mathrm{ann}_R(\mathcal{N})/\mathrm{ann}_R(\mathcal{N})^2\right)$ (see Ex. 12 of Chap. V.5 of [14]), where $\mathrm{ann}_R(\mathcal{N})/\mathrm{ann}_R(\mathcal{N})^2$ is the $R/\mathrm{ann}_R(\mathcal{N})$-module *conormal module*.

Example 4. In Example 3, we proved that $g_i = x_i$ for $i = 1, 2, 3$. Hence, if $D(x_i) := \Bbbk^{3 \times 1} \setminus V_{\Bbbk}(\langle x_i \rangle) = \{\psi = (\psi_1 \quad \psi_2 \quad \psi_3)^T \in \Bbbk^{3 \times 1} \mid \psi_i \neq 0\}$ for $i = 1, 2, 3$, then we have $\mathcal{P} = \bigcup_{i=1}^3 D(x_i)$. Moreover, we can check that

$$\begin{aligned}
\forall\, \psi \in D(x_1): \ E_{x_1}(\psi) &:= c^{-1} \begin{pmatrix} 0 & 0 & -\dfrac{1}{79\,\psi_1} \end{pmatrix}^T, \\
\forall\, \psi \in D(x_2): \ E_{x_2}(\psi) &:= (5956\,c)^{-1} \begin{pmatrix} -\dfrac{77}{\psi_2} & \dfrac{31}{\psi_2} & 0 \end{pmatrix}^T, \\
\forall\, \psi \in D(x_3): \ E_{x_3}(\psi) &:= (2978\,c)^{-1} \begin{pmatrix} \dfrac{29}{\psi_3} & \dfrac{27}{\psi_3} & 0 \end{pmatrix}^T,
\end{aligned}$$

are local right inverses of B, i.e., $B\,E_{\psi_i} = 1$, on $D(x_i)$ for $i = 1, 2, 3$. They are computed by the command LocalLeftInverse of the OreModules package [5]. Since $g := \gcd(g_1, g_2, g_3) = 1$, as shown above, $\mathrm{ann}_R(\mathcal{N})$ is not principal, and thus, no global right inverse E of B exists over the whole space $\mathcal{P}$. Using $\mathrm{ann}_R(\mathcal{N}) = \mathfrak{m}_0 = \langle x_1, x_2, x_3 \rangle$, the $R/\mathfrak{m}_0 \cong \Bbbk$-module $\mathfrak{m}_0/\mathfrak{m}_0^2$ is defined by the $\Bbbk$-linear combinations of the generators $\overline{x_i}$'s of $\mathfrak{m}_0/\mathfrak{m}_0^2$, where $\overline{x_i}$ denotes the residue class of x_i in $\mathfrak{m}_0/\mathfrak{m}_0^2$, i.e., $\mathfrak{m}_0/\mathfrak{m}_0^2 \cong \Bbbk^{3 \times 1}$, which shows that $t = \mu(\mathrm{ann}_R(\mathcal{N})) = 3$ is the least number of distinguished open sets of $\Bbbk^{3 \times 1}$ defining a cover of $\mathcal{P}$.

4.2 Existence of a local/global basis C of $\ker_R(B.)$

To study the local/global structure of the solution space (12) of (2), we now investigate the existence of a local/global basis $C(\psi)$ of $\ker(B(\psi).)$ over $\mathcal{P}$.

As explained in Section 3, a matrix $C \in R^{r \times s}$ can be computed satisfying $\ker_R(B.) = \mathrm{im}_R(C.)$ (use, e.g., the SyzygyModule command of the OreModules package). By construction, we have the exact sequence of R-modules:

$$0 \longleftarrow \mathcal{N} \xleftarrow{\ \kappa\ } R^{l \times 1} \xleftarrow{\ B.\ } R^{r \times 1} \xleftarrow{\ C.\ } R^{s \times 1}. \qquad (23)$$

Let $Q(R) := \Bbbk(x_1, \ldots, x_d)$ be the *field of fractions* of R, i.e., the field of rational functions in the x_i's with coefficients in $\Bbbk$ [7, 17]. The *rank* of a finitely generated R-module $\mathcal{L}$ is $\operatorname{rank}_R(\mathcal{L}) := \dim_{Q(R)} (Q(R) \otimes_R \mathcal{L})$. Since $\mathcal{N}$ is a torsion R-module, $\operatorname{rank}_R(\mathcal{N}) = 0$, the *Euler-Poincaré characteristic* applied to (14) yields $\operatorname{rank}_R(\ker_R(B.)) = r - l$ [7, 17], which yields $s \geq r - l$. The equality holds, i.e., $s = r - l$, iff $\ker_R(B.)$ is a *free* R-module, i.e., $\ker_R(B.) \cong R^{r-l}$ [17].

The problem of recognizing whether or not a module is free is an open question in module theory [14, 15, 17]. It can be effectively solved for $R = \Bbbk[x_1, \ldots, x_d]$ due to the *Quillen-Suslin theorem* [14, 15, 17]. The Quillen-Suslin theorem is implemented in the QuillenSuslin package [8]. Hence, we can effectively test whether or not $\ker_R(B.)$ is a free R-module and if so, compute a basis of $\ker_R(B.)$, namely, a full column rank matrix $C \in R^{r \times (r-l)}$ such that $\ker_R(B.) = \operatorname{im}_R(C.)$ [8]. We then have $\ker_{\Bbbk}(B(\psi).) = \operatorname{im}_{\Bbbk}(C(\psi).)$ for all $\psi \in \mathcal{P}$, i.e., C is a global basis of $\ker_R(B.)$ on $\mathcal{P}$. In particular, C is a local basis on $D(g_i)$ for all $i = 1, \ldots, t$. Using Theorems 1 and 2, we finally obtain that

$$\forall\, \psi \in D(g_i), \quad \forall\, Y' \in \Bbbk^{(r-l) \times m}, \quad \begin{cases} u = Z\, \psi, \\ v = \begin{pmatrix} E_{g_i}(\psi) & C(\psi) \end{pmatrix} \begin{pmatrix} Y \\ Y' \end{pmatrix}, \end{cases} \tag{24}$$

are solutions of (2) on $D(g_i)$. If $t = 1$, these solutions are globally defined on $\mathcal{P}$.

If $d = 1$, then $R = \Bbbk[x_1]$ is a principal ideal domain, which implies that $\operatorname{ann}_R(\mathcal{N}) = \langle g_1 \rangle$ and $\ker_R(B.)$ is a free R-module of rank $r - l$ [7, 17]. Let us show how to compute g_1, $E_{g_1} \in (S_{g_1}^{-1} R)^{r \times l}$ and a basis of $\ker_R(B.)$, i.e., a full column rank matrix $C \in R^{r \times (r-l)}$ satisfying $\ker_R(B.) = \operatorname{im}_R(C.)$. If we note $W := (W_1 \ \ldots \ W_r) \in \Bbbk^{l \times r}$, then we have $B = W\, x_1$. Hence, if $\psi_1 \neq 0$, then we get $\operatorname{rank}_{\Bbbk}(B(\psi_1)) = \operatorname{rank}_{\Bbbk}(W)$, which yields $\mathcal{P} = \emptyset$ if $\operatorname{rank}_{\Bbbk}(W) < l$, i.e., $g_1 = 0$, or $\mathcal{P} = \Bbbk \setminus \{0\}$ if $\operatorname{rank}_{\Bbbk}(W) = l$, i.e., $g_1 = x_1$. In the latter case, if $F \in \Bbbk^{r \times l}$ is a right inverse of W, i.e., $W\, F = I_l$, then $E_{g_1} = x_1^{-1}\, F$ is a right inverse of B. Moreover, let $C \in \Bbbk^{r \times (r-l)}$ be a matrix whose columns define a basis of $\ker_{\Bbbk}(W.)$. Then, we have $\ker_R(B.) = \operatorname{im}_R(C.) \cong R^{r-l}$. We note that E and C can be computed by standard linear algebra methods.

Example 5. Let us consider the following matrices:

$$D_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad D_2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad D_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

$$D_4 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad M = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

We can easily check that $l := \operatorname{rank}_{\Bbbk}(M) = 3$, $r = 4$ and:

$$X = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \ Y = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \ L = (1 \quad 0 \quad 0 \quad -1), \ Z = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$W_1 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \; W_2 = -\frac{1}{2} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{pmatrix}, \; W_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \; W_4 = -\frac{1}{2} \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 1 & 1 \end{pmatrix},$$

$$R = \Bbbk[x_1, x_2, x_3], \quad B = \begin{pmatrix} -x_1 & 0 & x_1 & 0 \\ 0 & -\frac{1}{2}(x_2 - x_3) & 0 & \frac{1}{2}(x_2 - x_3) \\ 0 & -\frac{1}{2}(x_2 + x_3) & 0 & -\frac{1}{2}(x_2 + x_3) \end{pmatrix}.$$

If $g_1 := x_1\,(x_2^2 - x_3^2)$, then $\operatorname{ann}_R(\mathcal{N}) = \langle g_1 \rangle$. Hence, $t = 1$ and $\mathcal{P} = \Bbbk^3 \setminus V_{\Bbbk}(\langle g_1 \rangle)$, where $V_{\Bbbk}(\langle g_1 \rangle) = \{x_1 = 0\} \cup \{x_2 - x_3 = 0\} \cup \{x_2 + x_3 = 0\}$. We can check that the R-module $\ker_R(B.)$ is free of rank 1, i.e., $\ker_R(B.) \cong R$. Using [4, 8], we get $\ker_R(B.) = \operatorname{im}_R(C.)$, where $C = (1 \quad 0 \quad 1 \quad 0)^T \in R^{4 \times 1}$. Finally, using the OreModules package, we obtain that the following matrix

$$E_{g_1} = \frac{1}{g_1} \begin{pmatrix} 0 & 0 & 0 \\ 0 & -x_1\,(x_2 + x_3) & -x_1\,(x_2 - x_3) \\ x_2^2 - x_3^2 & 0 & 0 \\ 0 & x_1\,(x_2 + x_3) & -x_1\,(x_2 - x_3) \end{pmatrix}$$

is a right inverse of B, i.e., $B\,E_{g_1} = I_3$. Hence, all the solutions of (2) with full row rank matrices v can be expressed by a single closed-form given by (24) with $t = 1$ and for all $\psi \in \mathcal{P}$ and for all $Y' = (y_1' \quad y_2' \quad y_3' \quad y_4') \in \Bbbk^{1 \times 4}$ such that:

$$\det((Y^T \quad Y'^T)^T) = y_4' - y_1' \neq 0.$$

Let us now suppose that the R-module $\ker_R(B.)$ is not free. Let us study the module structure of the $S_{g_i}^{-1}R$-module $\ker_{S_{g_i}^{-1}R}(B.)$. Since $S_{g_i}^{-1}R$ is a flat R-module, the functor $S_{g_i}^{-1}R \otimes_R \cdot$ is exact [7, 14, 17]. Hence, applying $S_{g_i}^{-1}R \otimes_R \cdot$ to (23) and using the fact that $S_{g_i}^{-1}R \otimes_R \mathcal{N} \cong S_{g_i}^{-1}\mathcal{N} = 0$, we get the following split exact sequence of $S_{g_i}^{-1}R$-modules [7, 17]:

$$0 \longleftarrow (S_{g_i}^{-1}R)^{l \times 1} \xleftarrow{B.} (S_{g_i}^{-1}R)^{r \times 1} \xleftarrow{C.} (S_{g_i}^{-1}R)^{s \times 1}.$$

See also Remark 9. Hence, we first obtain

$$\ker_{S_{g_i}^{-1}R}(B.) = \operatorname{im}_{S_{g_i}^{-1}R}(C.), \tag{25}$$

and then $(S_{g_i}^{-1}R)^r \cong (S_{g_i}^{-1}R)^l \oplus \ker_{S_{g_i}^{-1}R}(B.)$, which shows that $\ker_{S_{g_i}^{-1}R}(B.)$ is a *stably free* $S_{g_i}^{-1}R$-module of rank $r - l$ [17]. Thus, $\ker_{S_{g_i}^{-1}R}(B.)$ is not necessarily a free $S_{g_i}^{-1}R$-module. Recognizing whether or not a stably free $S_{g_i}^{-1}R$-module is free is an open question in module theory as well as the problem of computing bases of free $S_{g_i}^{-1}R$-modules. For more details, see, e.g., [15, 14, 17].

If $\ker_{S_{g_i}^{-1} R}(B.)$ is a free $S_{g_i}^{-1} R$-module of rank $r-l$, then there exists a full column rank matrix $C_{g_i} \in (S_{g_i}^{-1} R)^{r \times (r-l)}$ such that

$$\ker_{S_{g_i}^{-1} R}(B.) = \operatorname{im}_{S_{g_i}^{-1} R}(C_{g_i}.) \cong (S_{g_i}^{-1} R)^{(r-l)}, \tag{26}$$

i.e., the $r-l$ columns of the matrix C_{g_i} define a basis of the free $S_{g_i}^{-1} R$-module $\ker_{S_{g_i}^{-1} R}(B.)$. Hence, we obtain $\ker_{\Bbbk}(B(\psi).) = \operatorname{im}_{\Bbbk}(C_{g_i}(\psi).)$ for all $\psi \in D(g_i)$. Thus, C_{g_i} defines a basis of $\ker_R(B.)$ on $D(g_i)$. Theorems 1 and 2 then imply that the solutions of (2) defined on $D(g_i)$ are given by:

$$\forall\, \psi \in D(g_i), \quad \forall\, Y' \in \Bbbk^{(r-l)\times m}, \quad \begin{cases} u = Z\,\psi, \\ v = \begin{pmatrix} E_{g_i}(\psi) & C_{g_i}(\psi) \end{pmatrix} \begin{pmatrix} Y \\ Y' \end{pmatrix}. \end{cases} \tag{27}$$

A stably free module of rank 1 over a commutative ring is free [15]. Hence, (27) holds when $r = \operatorname{rank}_{\Bbbk}(M) + 1$. See [8] for the computation of C_{g_i}.

If $\ker_{S_{g_i}^{-1} R}(B.)$ is not a free $S_{g_i}^{-1} R$-module, then no full column rank matrix $C_{g_i} \in (S_{g_i}^{-1} R)^{r \times (r-l)}$ exists such that (26) holds, i.e., such that $\ker_{\Bbbk}(B(\psi).) = C_{g_i}(\psi)\, \Bbbk^{(r-l)\times 1}$ for all $\psi \in D(g_i)$. Hence, no basis of $\ker_{\Bbbk}(B(\psi).)$ exists on $D(g_i)$. But, using (25), we have the following solutions of (2), where $s > r-l$:

$$\forall\, \psi \in D(g_i), \quad \forall\, Y'' \in \Bbbk^{s\times m}, \quad \begin{cases} u = Z\,\psi, \\ v = \begin{pmatrix} E_{g_i}(\psi) & C(\psi) \end{pmatrix} \begin{pmatrix} Y \\ Y'' \end{pmatrix}. \end{cases} \tag{28}$$

Example 6. We consider again Examples 3 and 4. Using [8], we can check that $\ker_R(B.)$ is not a free R-module. Using the OreModules package, we get that

$$C := \begin{pmatrix} -58\,x_2 - 77\,x_3 & -79\,x_1 & 0 \\ -54\,x_2 + 31\,x_3 & 0 & -79\,x_1 \\ 0 & 54\,x_2 - 31\,x_3 & -58\,x_2 - 77\,x_3 \end{pmatrix}$$

is such that $\ker_R(B.) = \operatorname{im}_R(C.)$, i.e., the 3 columns of C generate the R-module $\ker_R(B.)$ of rank $r-l=2$. We get the solutions (28) of (2) on $D(g_i)$ for $i=1,2,3$.

Finally, we study if the solutions of (2) can be written as (27). As explained, the $S_{x_i}^{-1} R$-module $\ker_{S_{x_i}^{-1} R}(B.)$ is stably free of rank 2. Using Corollary 4.10 of [15], i.e., a variant of the Quillen-Suslin theorem for the *generalized Laurent polynomial ring* $S_{x_i}^{-1} R = R[x_i^{\pm 1}, x_j]_{1 \le j \ne i \le 3}$, $\ker_{S_{x_i}^{-1} R}(B.)$ is a free $S_{x_i}^{-1} R$-module of rank 2. Using an implementation of this result in the QuillenSuslin package, a basis of $\ker_{S_{x_i}^{-1} R}(B.)$ is defined by the columns of the matrix C_{x_i} defined by:

$$C_{x_1} = \begin{pmatrix} -79\,x_1 & 0 \\ 0 & -79\,x_1 \\ 54\,x_2 - 31\,x_3 & -58\,x_2 - 77\,x_3 \end{pmatrix},$$

$$C_{x_2} = \begin{pmatrix} -\dfrac{29\,x_2}{73680} - \dfrac{77\,x_3}{147360} & -\dfrac{6083\,x_1}{5956\,x_2} \\ -\dfrac{9\,x_2}{24560} + \dfrac{31\,x_3}{147360} & \dfrac{2449\,x_1}{5956\,x_2} \\ 0 & 1 \end{pmatrix}, \; C_{x_3} = \begin{pmatrix} -\dfrac{29\,x_2}{73680} - \dfrac{77\,x_3}{147360} & \dfrac{2291\,x_1}{2978\,x_3} \\ -\dfrac{9\,x_2}{24560} + \dfrac{31\,x_3}{147360} & \dfrac{2133\,x_1}{2978\,x_3} \\ 0 & 1 \end{pmatrix}.$$

Hence, we have $\ker_{\Bbbk}(B(\psi).) = \mathrm{im}_{\Bbbk}(C_{x_i}(\psi).) \cong \Bbbk^{2\times 1}$ for all $\psi \in D(g_i)$ and for $i = 1, 2, 3$, and (27) are solutions of (2) defined on the $D(g_i)$'s given in Example 4.

Finally, we emphasize that all the examples were computed with the `Maple` packages OreModules [5] and QuillenSuslin [8]. For more details, see:

https://who.rocq.inria.fr/Alban.Quadrat/MapleConference.

References

1. Barakat, M., Lange-Hegermann, M.: The `homalg` project. Computeralgebra-Rundbrief, **51**, 6–9 (2012), https://github.com/homalg-project/HomalgProject.jl.
2. Capdessus, C.: Aide au diagnostic des machines tournantes par traitement du signal. PhD thesis, University of Grenoble (1992)
3. Capdessus, C., Sidahmed, M.: Analyse des vibrations d'un engrenage : cepstre, corrélation, spectre. In: GRETSI **8**, 365–372. Saint Martin d'Hères (1991)
4. Chyzak, F., Quadrat, A., Robertz, R.: Effective algorithms for parametrizing linear control systems over Ore algebras. Applicable Algebra in Engineering, Communications and Computing, **16**, 319–376 (2005)
5. Chyzak, F., Quadrat, A., Robertz, R.: OreModules: A symbolic package for the study of multidimensional linear systems. In: LNCIS **352**, 233–264, Springer (2007)
6. Dagher, R., Hubert, E., Quadrat, A.: On the general solutions of a rank factorization problem arising in vibration analysis, submitted, 2021.
7. Eisenbud, D.: Commutative Algebra with a View Toward Algebraic Geometry. Springer (1995)
8. Fabiańska, A., Quadrat, A.: Applications of the Quillen-Suslin theorem to multidimensional systems theory. In Radon Series on Computation and Applied Mathematics **3**, 23–106, de Gruyter publisher (2007)
9. Greuel, G.-M., Pfister, G.: A Singular Introduction to Commutative Algebra. Springer, 2002, https://www.singular.uni-kl.de/
10. Hubert, E.: Amplitude and phase demodulation of multi-carrier signals: Application to gear vibration signals. PhD Thesis, Université de Lyon (2019)
11. Hubert, E., Barrau, A., El Badaoui, M.: New multi-carrier demodulation method applied to gearbox vibration analysis. In: Proceedings of ICASSP 2018, (2018)
12. Hubert, E., Bouzidi, B., Dagher, R., Barrau, A., Quadrat, A.: Algebraic aspects of the exact signal demodulation problem. In: Proceedings of *SSSC & TDS* (2019)
13. Hubert, E., Bouzidi, B., Dagher, R., Barrau, A., Quadrat, A.: On a rank factorisation problem arising in gearbox vibration analysis. In: Proceedings of *IFAC World Congress* (2020)
14. Kunz, E.: Introduction to Commutative Algebra and Algebraic Geometry. Birkhäuser (1985)
15. Lam, T. Y.: Serre's Problem on Projective Modules. Springer (2006)
16. Quadrat, A.: An introduction to constructive algebraic analysis and its applications. Les cours du CIRM, **1**: Journées Nationales de Calcul Formel, 281–471 (2010)
17. Rotman, J. J.: Introduction to Homological Algebra. Springer (2009)